

REMARKS

In the Office Action, Claims 1-35 were examined and stand rejected. In response, Claims 1, 6, 21, and 26 are amended, Claims 31-35 are cancelled and no claims are added. Applicant respectfully requests reconsideration of pending Claims 1-35 in view of the following remarks.

I. Claims Rejected Under 35 U.S.C. §103

The Examiner rejects Claims 1-2, 5-7, 10-15, 17-32 and 34-35 under 35 U.S.C. §103 as being anticipated by U.S. Patent No. 5,809,148 issued to Doberstein et al. ("Doberstein") in view of U.S. Patent No. 5,259,025 issued to Monroe et al. ("Monroe"). Applicant respectfully traverses this rejection.

Claim 1 recites:

reading an encrypted data block from memory;
regenerating, within a time required to read the encrypted data block from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory; and
once reading of the encrypted data block is complete, decrypting the encrypted data block according to the generated keystream. (Emphasis added.)

While Applicant's argument here is directed to the cited combination of references, it is first necessary to first consider their individual teachings, to ascertain (if any) could be made from the cited references to Doberstein and Monroe.

Doberstein is generally directed to a method for decrypting retransmitted, encrypted data, where the retransmission does not include the entire message. (See col. 3, lines 4-6.) In contrast with Claim 1, Doberstein does not disclose or suggest reading an encrypted data block from memory, much less the regeneration of a keystream used to encrypt the data block within a predetermined time required to read the encrypted data block from the memory using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory, as in Claim 1. Doberstein does disclose the ability to decrypt selected parts of a message without unnecessary delays or redundant work, such as waiting for retransmission of an entire message or redecrypting data to decrypt the entire message (see col. 3, lines 16-20),

however, that is something completely different from regenerating a keystream used to encrypt a data block within a predetermined time required to read the encrypted data block from a memory by using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory, as in Claim 1.

The Examiner indicates that Doberstein is not clear in showing whether or not the block of encrypted data is read from storage before the retransmission process. (See page 3, first para. of the Office Action mailed 8/31/07.) We respectfully disagree with the Examiner's assertions and characterizations regarding Doberstein.

We submit that Doberstein cannot disclose or suggest that the retransmitted block is read from memory since any block within memory would not be stored in the encrypted format used by the encrypted communications system of Doberstein and any error-free retransmitted data blocks are available once the data block is received without error and decrypted prior to memory storage. (See process blocks 215-219 of FIG. 2 of Doberstein.) Apposite to Claim 1, Doberstein is expressly limited to the encryption of data for transmission and hence only stores decrypted data within memory. Doberstein explicitly requires that the keystream is either pulled from storage or generated from data stored from the initial receipt of the encrypted data message subsequent to receipt of the retransmitted data blocks without error (see col. 3, lines 12-16 and process block 219 of FIG. 2), however, that is something completely different from regenerating a keystream used to encrypt a data block within a predetermined time required to read the encrypted data block from a memory by using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory, as in Claim 1.

The Examiner relies on Monroe to rectify the deficiencies of Doberstein to disclose or suggest regenerating, within a time required to read the encrypted data block from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block, as in Claim 1. According to the Examiner, Monroe clearly teaches that the block of encrypted data is read from storage before a retransmission process at FIG. 4, element 94, and col. 1, lines 57-61 of Monroe. (See Supra.) Although process block 94 of FIG. 4 of Monroe and col. 1, lines 56-61 indicate that a video data table is read from a memory read of a presented user identification device, we submit that no combination of Doberstein in view of Monroe can teach

or suggest regenerating, within a time required to read the encrypted data block from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory, as in Claim 1.

Hence, no combination of Doberstein in view of Monroe could teach or suggest reading an encrypted data block from memory and regenerating a keystream used to encrypt the data block according to one or more stored criteria of the data block using a predetermined number of rounds of a cipher that are reduced to match a memory read latency of the memory, as in Claim 1

For each of the above reasons, therefore, Claim 1 and all claims which depend from Claim 1, are patentable over the cited prior art combination of Doberstein in view of Monroe as well as the references of record.

Each of Applicant's other independent claims include features similar to those highlighted above with reference to Claim 1 and therefore also patentable over the cited prior art combination of Doberstein in view of Monroe as well as the references of record for similar reasons.

Consequently, Applicants respectfully request that the Examiner reconsider and withdraw the §103(a) rejection of Claims 1-2, 5-7, 10-15, and 17-30.

DEPENDENT CLAIMS

In view of the above remarks, a specific discussion of the dependent claims is considered to be unnecessary. Therefore, Applicant's silence regarding any dependent claim is not to be interpreted as agreement with, or acquiescence to, the rejection of such claim or as waiving any argument regarding that claim.

II. Allowable Subject Matter

The Examiner has indicated that Claims 4, 9, 16 and 33 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form, including all of the limitations of the base claim and any intervening claims.

Regarding Claims 4, 9, 16 and 33, Claims 4, 9, 16 and 33 are also novel based on their dependency from Claims 1, 6, 11 and 31, respectively, for at least the reasons indicated above. Accordingly, Applicant respectfully requests that the Examiner allow Claims 4, 9, 16 and 33, based on their dependency from Claims 5, 6, 11 and 31, respectively.

CONCLUSION

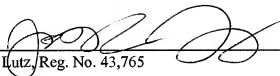
In view of the foregoing, it is believed that all claims now pending (1) are in proper form, (2) are neither obvious nor anticipated by the relied upon art of record, and (3) are in condition for allowance. A Notice of Allowance is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, the Examiner is encouraged to contact the undersigned at (310) 207-3800.

If necessary, the Commissioner is hereby authorized in this, concurrent and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly, extension of time fees.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR, & ZAFMAN LLP

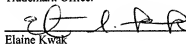
Dated: 10/29/07

By: 
Joseph Lutz, Reg. No. 43,765

1279 Oakmead Parkway
Sunnyvale, California 94085-4040
Telephone (310) 207-3800
Facsimile (408) 720-8383

CERTIFICATE OF TRANSMISSION

I hereby certify that this correspondence is being submitted electronically via EFS Web on the date shown below to the United States Patent and Trademark Office.

 10/29/07
Elaine Kwak Date